Billing Code 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 130909789-3789-01]

Request for Comments on the Preliminary Cybersecurity Framework

AGENCY: National Institute of Standards and Technology (NIST), Department of Commerce.

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) seeks comments on the preliminary version of the Cybersecurity Framework ("preliminary Framework"). The preliminary Framework was developed by NIST using information collected through the Request for Information (RFI) that was published in the Federal Register on February 26, 2013, and a series of open public workshops. The preliminary Framework was developed in response to NIST responsibilities directed in Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" ("Executive Order"). Under the Executive Order, the Secretary of Commerce is tasked to direct the Director of NIST to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework" or "Framework"). The Framework will consist of standards, methodologies, procedures

and processes that align policy, business, and technological approaches to address cyber risks. The preliminary Framework is available electronically from the NIST Web site at: http://www.nist.gov/itl/cyberframework.cfm.

DATES: Comments must be received by 5:00 PM Eastern Time **[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Both written and electronic comments should be submitted using the comment template form available electronically from the NIST Web site at: http://www.nist.gov/itl/cyberframework.cfm. Written comments concerning the preliminary Framework may be sent to: Information Technology Laboratory, ATTN: Adam Sedgewick, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930. Electronic comments concerning the preliminary Framework should be submitted in Microsoft Word or Excel formats to: csfcomments@nist.gov, with the Subject line: Preliminary Cybersecurity Framework Comments.

The preliminary Cybersecurity Framework is available electronically from the NIST Web site at: http://www.nist.gov/itl/cyberframework.cfm.

FOR FURTHER INFORMATION CONTACT: Diane Honeycutt, telephone: 301-975-8443, National Institute of Standards and Technology, 100 Bureau Drive, Stop

8930, Gaithersburg, MD 20899-8930 or via email: dhoneycutt@nist.gov. Please direct media inquiries to NIST's Public Affairs Office at (301) 975-NIST.

SUPPLEMENTARY INFORMATION:

The national and economic security of the United States depends on the reliable functioning of critical infrastructure,[1] which has become increasingly dependent on information technology. Recent trends demonstrate the need for improved capabilities for defending against malicious cyber activity. Such activity is increasing, and its consequences can range from theft through disruption to destruction. Steps must be taken to enhance existing efforts to increase the protection and resilience of this infrastructure, while maintaining a cyber environment that encourages efficiency, innovation, and economic prosperity, while protecting privacy and civil liberties.

Under the Executive Order,[2] the Secretary of Commerce is tasked to direct the Director of NIST to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework" or "Framework"). The Cybersecurity Framework will consist of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber

[1] For the purposes of this notice the term "critical infrastructure" has the meaning given the term in 42 U.S.C 5195c(e), "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[2] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11739 (February 19, 2013).

risks. Given the diversity of sectors in critical infrastructure, the Framework development process was designed to initially identify cross-sector security standards and guidelines that are immediately applicable or likely to be applicable to critical infrastructure, to increase visibility and adoption of those standards and guidelines, and to find potential areas for improvement (i.e., where standards/guidelines are nonexistent or where existing standards/guidelines are inadequate) that need to be addressed through future collaboration with industry and industry-led standards bodies. The Cybersecurity Framework will incorporate voluntary consensus standards and industry best practices to the fullest extent possible and will be consistent with voluntary international consensus-based standards when such international standards advance the objectives of the Executive Order. The Cybersecurity Framework will be designed for compatibility with existing regulatory authorities and regulations.

The Cybersecurity Framework will provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will not prescribe particular technological solutions or specifications. It will include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework and will include methodologies to identify and mitigate impacts of the Framework and associated information security measures and controls on business confidentiality and to protect individual privacy and civil liberties.

As a non-regulatory Federal agency, NIST developed the preliminary Framework in a manner that is consistent with its mission to promote U.S. innovation and industrial competitiveness through the development of standards and guidelines in consultation with stakeholders in both government and industry. The preliminary Framework seeks to provide owners and operators of critical infrastructure the ability to implement security practices in the most effective manner while allowing organizations to express requirements to multiple authorities and regulators. Issues relating to harmonization of existing relevant standards and integration with existing frameworks were also considered. While the focus is on the Nation's critical infrastructure, the preliminary Framework was developed in a manner to promote wide adoption of practices to increase cybersecurity across all sectors and industry types.

The preliminary Framework was developed through an open public review and comment process that included information collected through Request for

Information (RFI), 78 FR 13024 (February 26, 2013), and a series of public workshops. Comments received in response to the RFI are available at http://csrc.nist.gov/cyberframework/rfi_comments.html.

NIST held four open public workshops to provide the public with additional opportunities to provide input. The first workshop was conducted on April 3, 2013, at the Department of Commerce in Washington, D.C. The second workshop was conducted on May 29-31, 2013, at Carnegie Mellon University in Pittsburgh, Pennsylvania. The third workshop was conducted on July 10-12, 2013, at the University of California, San Diego. The fourth workshop was conducted on September 11-13, 2013, at the University of Texas at Dallas. Agenda, discussion materials, and presentation slides for each of these workshops are available at http://www.nist.gov/itl/cyberframework.cfm.

Throughout the process, NIST issued public updates on the development of the Cybersecurity Framework. NIST issued the first update on June 18, 2013, and it is available at http://www.nist.gov/itl/upload/nist_cybersecurity_framework_update_061813.pdf. NIST issued the second update on July 24, 2013, and it is available at http://www.nist.gov/itl/upload/NIST-Cybersecurity-Framework-Update-072413.pdf.

The preliminary Framework incorporates existing consensus-based standards to the fullest extent possible, consistent with requirements of the National Technology Transfer and Advancement Act of 1995,[3] and guidance provided by Office of Management and Budget Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities."[4] Principles articulated in the Executive Office of the President memorandum M-12-08 "Principles for Federal Engagement in Standards Activities to Address National Priorities"[5] are followed. The preliminary Framework is also consistent with, and supported by the broad policy goals of, the Administration's 2010 "National Security Strategy,"[6] 2011 "Cyberspace Policy Review,"[7] "International Strategy for Cyberspace"[8] of May 2011 and HSPD-7 "Critical Infrastructure Identification, Prioritization, and Protection."[9]

Request for Comments:

NIST seeks public comments on the preliminary Cybersecurity Framework. The draft report is available electronically from the NIST Web site at: http://www.nist.gov/itl/cyberframework.cfm. The comment templates are available at the same address, and are required for both written and electronic comments.

[3] Public Law 104-113 (1996), codified in relevant part at 15 U.S.C 272(b).
[4] http://www.whitehouse.gov/omb/circulars_a119
[5] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf
[6] http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
[7] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[8] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[9] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf

Interested parties should submit comments in accordance with the DATES and ADDRESSES sections of this notice. All comments will be posted at http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or business information).

Dated: October 23, 2013.

Patrick Gallagher,
Under Secretary of Commerce for Standards and Technology .

[FR Doc. 2013-25566 Filed 10/28/2013 at 8:45 am; Publication Date: 10/29/2013]